What is claimed is:

1. An apparatus authentication system which comprises a server apparatus and a client apparatus which perform a mutual authentication when a content is transmitted from the server apparatus to the client apparatus for use therein, wherein

the client apparatus includes:

a receiving unit operable to receive challenge data from the server apparatus;

a signature generating unit operable to generate signature data based on the received challenge data and a first password; and

a transmitting unit operable to transmit the generated signature data, and

the server apparatus includes:

a challenge data transmitting unit operable to generate and transmit the challenge data;

a holding unit operable to hold a second password in advance;

a receiving unit operable to receive the signature data from the client apparatus;

an authentication unit operable to perform an authentication of the received signature data based on the challenge data and the second password; and

a content transmitting unit operable to, if the authentication results in success, transmit an encrypted content to the client apparatus, the encrypted content having been encrypted in such a manner that the encrypted content can be decrypted by the client apparatus.

2. A server apparatus for transmitting a content to a client apparatus, comprising:

a holding unit operable to hold a registered password;

a challenge data transmitting unit operable to generate and transmit challenge data;

a receiving unit operable to receive, from the client apparatus, signature data that has been generated based on a password and the challenge data;

an authentication unit operable to perform an authentication of the received signature data based on the registered password and the challenge data; and

a content transmitting unit operable to, if the authentication results in success, transmit an encrypted content to the client apparatus, the encrypted content having been encrypted in such a manner that the encrypted content can be decrypted by the client apparatus.

3. The server apparatus of Claim 2 further comprising

a registering unit operable to register a password, which is input from outside the server apparatus, with the holding unit as the registered password.

4. The server apparatus of Claim 2 further comprising:

a distance judging unit operable to detect a communication distance between the server apparatus and the client apparatus, and judge whether the detected communication distance is within a predetermined range of values; and

a registering unit operable to, if the distance judging

unit judges that the detected communication distance is within the predetermined range of values, register a password, which is transmitted from the client apparatus, with the holding unit as the registered password.

5. The server apparatus of Claim 2, wherein

the holding unit holds a first password and a second password that has a greater number of characters than the first password, and

the authentication unit includes:

a distance detecting sub-unit operable to detect a communication distance between the server apparatus and the client apparatus;

a password selecting sub-unit operable to select the first password if the detected communication distance is shorter than a predetermined communication distance, and select the second password if the detected communication distance is not shorter than the predetermined communication distance; and

an authentication sub-unit operable to perform the authentication of the received signature data based on the challenge data and the selected password as the registered password.

6. A client apparatus for receiving a content from a server apparatus and reproducing the received content, comprising:

a receiving unit operable to receive challenge data from the server apparatus;

a signature generating unit operable to generate signature

data based on the received challenge data and a first password;

a transmitting unit operable to transmit the generated signature data to the server apparatus; and

a content receiving unit operable to, if an authentication of the signature data results in success in the server apparatus, receive an encrypted content from the server apparatus, the encrypted content having been encrypted in such a manner that the encrypted content can be decrypted by the client apparatus.

7. The client apparatus of Claim 6 further comprising

a password receiving unit operable to receive a password which is input from outside, wherein

the transmitting unit transmits the received password to the server apparatus, and

the server apparatus receives and stores the password as a registered password.

8. The client apparatus of Claim 7 further comprising

a distance detecting unit operable to detect a communication distance between the client apparatus and the server apparatus, wherein

the transmitting unit transmits the received password to the server apparatus if the detected communication distance is shorter than a predetermined communication distance.

9. The client apparatus of Claim 6, wherein

a password of the client apparatus has been registered with a server apparatus in advance,

the transmitting unit generates and transmits authentication challenge data to the server apparatus before the content receiving unit receives the encrypted content from the server apparatus,

the content receiving unit receives, before receiving the encrypted content, server signature data that is generated by the server apparatus based on the transmitted authentication challenge data and a first server password held by the server apparatus,

the client apparatus further comprising:

a password holding unit operable to acquire a second server password from the server apparatus with which the password of the client apparatus has been registered, and hold the acquired second server password; and

an authentication unit operable to perform an authentication of the received server signature data based on the authentication challenge data and the second server password, wherein

the content receiving unit receives the encrypted content from the server apparatus if the authentication of the server signature data results in success.

10. The client apparatus of Claim 6 further comprising a user authentication unit which includes:

a storage sub-unit operable to store, in advance, first authentication data which is generated by extracting features of first unique information that is a characteristic an authorized user has uniquely as a living being;

an information receiving sub-unit operable to receive second unique information input by a user, the second unique information being a characteristic unique to the user as a living being;

a feature extracting sub-unit operable to generate second authentication data by extracting features of the second unique information; and

a judging sub-unit operable to judge whether a rate of match between the first authentication data and the second authentication data exceeds a predetermined value, wherein

the signature generating unit generates the signature data if the user authentication unit judges that the rate of match exceeds the predetermined value.

11. An apparatus authentication system which comprises a server apparatus and a client apparatus which perform a mutual authentication when a content is transmitted from the server apparatus to the client apparatus for use therein, wherein

the client apparatus includes:

a receiving unit operable to receive challenge data from the server apparatus;

a signature generating unit operable to generate signature data based on the received challenge data and authentication data which is generated based on a characteristic of a user of the client apparatus that the user has uniquely as a living being; and

a transmitting unit operable to transmit the generated signature data, and

the server apparatus includes:

a challenge data transmitting unit operable to generate and transmit the challenge data;

a holding unit operable to hold, in advance, registered data which is generated based on a characteristic that an authorized user, who is authorized to use contents, has uniquely as a living being;

a receiving unit operable to receive the signature data from the client apparatus;

an authentication unit operable to perform an authentication of the received signature data based on the challenge data and the registered data; and

a content transmitting unit operable to, if the authentication results in success, transmit an encrypted content to the client apparatus, the encrypted content having been encrypted in such a manner that the encrypted content can be decrypted by the client apparatus.

12. A method for use in a server apparatus that transmits a content to a client apparatus, wherein

the server apparatus holds a registered password,

the method comprising:

a challenge data transmitting step for generating and transmitting challenge data;

a receiving step for receiving, from the client apparatus, signature data generated based on a password and the challenge data;

an authentication step for performing an authentication

of the received signature data based on the registered password and the challenge data; and

a content transmitting step for, if the authentication results in success, transmitting an encrypted content to the client apparatus, the encrypted content having been encrypted in such a manner that the encrypted content can be decrypted by the client apparatus.

13. A program for use in a server apparatus that transmits a content to a client apparatus, wherein

the server apparatus holds a registered password,

the program comprising:

a challenge data transmitting step for generating and transmitting challenge data;

a receiving step for receiving, from the client apparatus, signature data generated based on a password and the challenge data;

an authentication step for performing an authentication of the received signature data based on the registered password and the challenge data; and

a content transmitting step for, if the authentication results in success, transmitting an encrypted content to the client apparatus, the encrypted content having been encrypted in such a manner that the encrypted content can be decrypted by the client apparatus.

14. A computer-readable recording medium which records therein a program for use in a server apparatus that transmits

a content to a client apparatus, wherein

the server apparatus holds a registered password,

the program comprising:

a challenge data transmitting step for generating and transmitting challenge data;

a receiving step for receiving, from the client apparatus, signature data generated based on a password and the challenge data;

an authentication step for performing an authentication of the received signature data based on the registered password and the challenge data; and

a content transmitting step for, if the authentication results in success, transmitting an encrypted content to the client apparatus, the encrypted content having been encrypted in such a manner that the encrypted content can be decrypted by the client apparatus.

15. A method for use in a client apparatus that receives a content from a server apparatus and reproduces the received content, the method comprising:

a receiving step for receiving challenge data from the server apparatus;

a signature generating step for generating signature data based on the received challenge data and a password;

a transmitting step for transmitting the generated signature data to the server apparatus; and

a content receiving step for, if an authentication of the signature data results in success in the server apparatus,

receiving an encrypted content from the server apparatus, the encrypted content having been encrypted in such a manner that the encrypted content can be decrypted by the client apparatus.

16. A program for use in a client apparatus that receives a content from a server apparatus and reproduces the received content, the program comprising:

a receiving step for receiving challenge data from the server apparatus;

a signature generating step for generating signature data based on the received challenge data and a password;

a transmitting step for transmitting the generated signature data to the server apparatus; and

a content receiving step for, if an authentication of the signature data results in success in the server apparatus, receiving an encrypted content from the server apparatus, the encrypted content having been encrypted in such a manner that the encrypted content can be decrypted by the client apparatus.

17. A computer-readable recording medium which records therein a program for use in a client apparatus that receives a content from a server apparatus and reproduces the received content, the program comprising:

a receiving step for receiving challenge data from the server apparatus;

a signature generating step for generating signature data based on the received challenge data and a password;

a transmitting step for transmitting the generated

signature data to the server apparatus; and

a content receiving step for, if an authentication of the signature data results in success in the server apparatus, receiving an encrypted content from the server apparatus, the encrypted content having been encrypted in such a manner that the encrypted content can be decrypted by the client apparatus.